Effective Food Security Plans for Production Agriculture and Food Processing

Gleyn E. Bledsoe, PhD, CPA, Department of Biological Systems Engineering;
Barbara A. Rasco, PhD, JD, Department of Food Science and Human Nutrition
Washington State University

Abstract

A model for developing a food security program derived from HACCP principles and applicable to production agriculture, food processing, food distribution, or food service which interfaces with current HACCP (21 CFR Part 123), GMP (21 CFR Part 110) and recall (21 CFR Part 7) programs is presented. Implementation strategies and developmental approaches are described including investment tax credits as a means of providing funding for implementation of these programs in the private sector.

Introduction

The events of September 11, 2001 focused the nation's and the world's attention on terrorism and the threat of future terrorist acts. Until the recent mail attacks involving anthrax, the media's focus on bioterrorism has involved the potential use of biological weapons (weapons of mass destruction) by international terrorist organizations. However, as we are all well aware, the use of anthrax or other pathogenic agents on even a relatively small scale can rapidly overwhelm the response mechanisms in place to deal with the perceived threat.

Even though weapons of mass destruction remain a potential threat, in our opinion, this is not the major risk to food systems or to the public at large because these agents are relatively difficult to stabilize, transport and effectively disseminate on a large scale. A simpler and more likely form of attack involves limited or individual use of pathogens developed specifically for biological warfare purposes as well as common bacterial foodborne or zoonotic agents. Zoonotics are animal diseases [(*e.g*. anthrax (*Bacillus anthracis*), plague (*Yersinia pestis*) and rabbit fever (*Franciscella tularensis*)] that can be transmitted to humans. Other possible risks involve economic terrorism targeted at a specific commercial entity or industry segment involving the real or threatened introduction of an animal or plant pathogen (or its genetic material) at production or agricultural facility. This would also include the actual or threatened introduction of genetic material(s) into products.

The Impact of Small Strategic Attacks

Groups with limited resources could perpetrate an attack employing any of these agents. As seen with the anthrax "mail bombs" in October 2001, even limited small-scale terrorist activities can rapidly saturate the emergency response and

medical facilities of a community. The response to the anthrax "mail bombs" in Washington, DC, New York, and Florida tied up investigative and response agencies across the nation. Because of enhanced screening and treatment, mail deliveries to Washington DC remained slow over three months after the anthrax scares. Some affected government offices remain closed as of January 2002, and have received expensive sanitation treatments with chlorine dioxide and other agents. Precautionary responses to numerous false alarms across the nation, such as the anthrax scares in Nevada, employed large number of police, fire and hazardous materials response teams. Even the post office in our small community of Pullman, WA (population: 25,000) was closed for several hours on a Friday afternoon when a damaged package began leaking white powder (potato starch). The response involved the entire on-duty police force and fire department, two ambulances, the WSU Environmental Health Department HAZMAT team and, naturally, two TV news camera crews from Spokane, about 90 miles away.

To further complicate matters, acts of bioterrorism may occur and not be detected by authorities or detected in a timely manner. What many individuals consider the only real recent case of intentional mass food poisoning in the United States occurred in September 1984. In this case, members of the Rajneeshee cult contaminated salad bars with salmonella (*Salmonella typhimurium*) in the small regional hub of The Dalles, Oregon, a city on the Columbia River. Over 1000 individuals reported symptoms, with 751 confirmed cases.

Despite several laboratory confirmations of the same pathogenic strain, two confirmed outbreaks (September 9th and 25th), reported illnesses from individuals who had eaten at ten separate restaurants, and suspicions advanced by a local authorities (Judge William Hulse); the deputy State epidemiologist concluded in his November 1984 report that there was no evidence to support the hypothesis that the outbreak was the result of deliberate contamination. Instead the epidemiologist stated that the contamination “could have occurred where food handlers failed to wash their hands adequately after bowel movements and then touched raw foods.”

This misconception received further support from the Epidemic Intelligence Service of the U.S. Center for Disease Control and Prevention, in its report issued in January 1985 that stated it, too, “was unable to find the source of the outbreaks and that food handlers were probably to blame”. Because workers preparing the food at the affected restaurants had fallen ill before most patrons had, the report reasoned, and because some minor violations of sanitary practices at few restaurants had been detected, food handlers “may have contaminated” the salad bars, the CDC concluded. Again the CDC asserted that there was “no epidemiologic evidence” to suggest that the contamination had been deliberate.” It was not until September 16, 1985, a year after the outbreaks, that law enforcement officials conducted a criminal investigation of the incident, and only then after the leader of the Raneeshees alerted officials that rogue members of his group had deliberately perpetrated this act of bioterrorism (Miller, 2001).

Definitions

Terrorism is commonly defined as the use of force or violence against persons or property in violation of criminal laws for the purpose of intimidation, coercion or ransom (FEMA, 1998). The intent of terrorism is to cause property damage, physical injury, or economic damage to people or to an entity such as a corporation or research institute. *Biological terrorism* or "*bioterrorism*" involves the use of etiologic or biological toxin agents in a terrorist act. The term *bioterrorism* has commonly been applied to acts of ecoterrorism as well, since ecoterrorism often involves biological targets (*e.g*. plots of allegedly genetically modified crops) or ecosystem issues (*e.g*. forest practices, biodiversity, sustainable agriculture).

In response to terrorist threats to the food supply, antiterrorism and counter-terrorism strategies will be employed. *Anti-terrorism* covers defensive measures used to reduce the vulnerability of individuals and property to terrorist acts while *counter-terrorism* refers to offensive measures to prevent, deter, and respond to terrorism. Currently the term "biodefense" is the buzzword used to encompass both "anti" and "counter"- terrorism activities.

Motivation and Likely Perpetrators

The threat of a food-tampering incident involving harmless materials (or no materials) can be as effective as a real attack. Simply claiming that a product as been purposely contaminated with dangerous material is sufficient to precipitate an extensive product recall with the associated adverse publicity, short-term economic loss and longer-term loss of market share and the resultant economic impact. For example, a Class I recall is required when there is: " a reasonable probability that the use of or exposure to a violative product will cause adverse health consequences or death." (21 CFR §7.3(m)(1)).

The most likely perpetrators of terrorist activity targeting the food industry have a variety of different motivations. The motivation can be economic (targeted to financially impact a specific commercial entity or industry segment) to political (making a "statement," influencing the outcome of an election, or forcing a particular political outcome) to malicious mischief (the infamous "copy-catter").

The most probable perpetrators are groups promoting causes with a degree of public support. Many individuals engaged in food terrorism may initially have been well- intentioned activists from animal rights, consumer protection, and environmental conservation movements. Still others may come from groups threatened by innovation. Commonly, bio- or eco- terrorists are anarchist factions tied directly or indirectly to mainstream groups that reasonably and peaceably strive to promote their political causes (Washington, 2001).

These "spin-off" terrorist factions typically form loosely organized, fluid networks or cells with anonymous memberships. They carefully research their targets, and employ increasingly sophisticated tactics for directed attacks. Their motivation is directed towards the elimination of real or imagined injustices. Facts are irrelevant and normally do not inhibit the activities of these extremist factions.

Threat from terrorists and terrorist groups against food research, production and processing are increasing. Actions by these groups can be extremely well organized and orchestrated commonly employing both overt and covert methodology to damage or destroy property or commerce, threaten public health and safety, and threaten, torment or injure people (Hollingsworth, 2001).

Examples of Targets and Strategies

The types of attacks terrorists have directed against the food industry to date range from false statements or accusations to overt acts designed to destroy property, information and communication systems, crops, animals, and people (Washington, 2001). Product tampering (real or hoaxes) and vandalism have proven to be particularly “productive” in terms of perpetrator notoriety and economic damage to targets. Such food terrorism is directed against perceived injustices and while their actions are not necessarily encompassed within the realm of conventional terrorist activities the results often are. On a larger scale, attacks against a country’s crops and livestock remain a viable aggressive weapon in the strategic planning of many governments, particularly those with reduced conventional weaponry.

Objectives of food terrorism include: the desire to severely impact a company and put it out of business by affecting the stock price or product availability or marketability in a malicious way; a program directed towards the elimination of a specific food, ingredient or agricultural practice; prohibit the importation of competing crops, research or development in a particular area; and pressure to erect trade barriers.

Many food terrorism methods are cheap and simple, such as flooding a company by mail, phone or electronically with harassing correspondence or repeated requests for information, filing consumer complaints, and entering tampering threats. Other tactics may include: spurious complaints to regulatory agencies, media “tips”, filing frivolous law suits, boycotts, lock-outs, and publicity stunts. Unfortunately bombings, fire, product tampering including poisonings, crop destruction, vandalism, or the threats of all of these, and finally targeted harassment of employees, suppliers and customers are also becoming tactics that are all too commonly employed.

Agriculture production (including food, fiber and paper) and the associated processing industries have been popular targets of bio or eco terrorists. There seems to be no segment immune to attack. Some extremist groups are violently

opposed to the development of natural resources, others, the “imprisonment and exploitation” of animals, and the use of meat and fur. Food and agricultural companies have also been targeted for using or developing genetically modified organisms. Specific targets include: primary producers, processors, distributors, retailers, shareholders, consumers, vendors/suppliers and researchers. Corporations, in particular, are considered by most terrorist groups to be nonstate and/or metastate entities and therefore legitimate targets of aggression in their own right based on this alone (Bascetta, 2000). Universities are deemed culpable through their association with private corporations or corporate foundations. Government research facilities are targeted by groups seeking to make a political "statement" against an unpopular governmental policy, or for the alleged failure of a governmental agency to take certain types of action which would further the causes of their group.

Thousands of products each year are subject to malicious tampering and accidental contamination which would precipitate a product recall or market withdrawal (Hollingsworth, 2001; Washington, 2001). Food, beverages, pharmaceuticals, agricultural chemicals, fertilizers, pest control media, and genetically modified crops are among the products more commonly affected. Activities directed specifically against organizations supporting or of being directly involved with biotechnology are facing threats that mirror these (Bledsoe and Rasco, 2001). Food contamination case and precautionary recalls are looming possibilities and are a major motivating force behind the stringent process controls and quality assurance procedures in the food industry. However, crisis management planning will take on different twists as food becomes more political, as international markets grow, and as price sensitivity increases (Hollingsworth, 2000).

Current Level of Readiness

Most organization are ill prepared to deal with tampering incidents let alone other manifestations of bioterrorism. Issues of product liability, insurance coverage issues, crisis management and maintaining business viability are of critical concern. A focus here, and in recent conferences is on analyzing an organization’s risk before an incident occurs, utilizing best practices to avoid a tampering or contamination event, formulating and instituting a crisis management and communication plan, conducting a cost and benefit analysis for transferring the risk through insurance coverage, conducting product recalls, litigating a tampering or recall case, forensic accounting to quantify losses and analyze claims. (ACI, 2000).

High profile consumer product tampering instances from the 1980’s made companies aware of new risks, however, we have unfortunately entered a brave new world of well organized, internationally based, targeting of organizations, and products in and related to the food industry. Recent conferences have addressed techniques for monitoring open-space research, covert sensor technology, and crime prevention training (ACI, 2000). According to the FBI, domestic crime

targeting biotechnology is the emerging anti-technology crime of the new millenium. (FBI, 2000). However, techniques and tools for protecting, monitoring open space research areas and facilities are limited (FBI, 2000).

Although twenty-two states have recently passed legislation increasing the penalties for malicious acts directed food and agricultural facilities, the effectiveness of these laws is yet to be seen (Anon. 2002).

Government Response

In response to the September 11, 2001 attack and the subsequent biological terrorist attack employing anthrax (*Bacillus anthracis*), several federal agencies, most notably the Food and Drug Administration (FDA), have introduced "guidance documents" which most likely will evolve into *de facto* or actual regulations governing food security. In addition, House Bill 3448 Public Health Security and Bioterrorism Response Act of 2001 was approved by the House on December 11, 2001, received by the Senate on December 18, 2001 and is currently in a conference committee with legislation likely this spring.

The net effect, the food industry of the United States, from producer to the table, can look forward to increased regulation and operating costs. The industry might well benefit from being proactive in this area. To be so enables the industry to guide the direction of regulation rather than to be forced into a position of reaction and defense. This paper proposes such a proactive approach in the form of legislative efforts to address physical security and human resource vetting as related to improving food security.

The first proposal, in regards to physical security, would require each food producer, manufacturer, distributor, and transportation company to conduct a food security hazard analysis followed by the preparation and implementation of a written security plan. This plan would incorporate the company's Hazard Analysis Critical Control Point (HACCP) plan, Sanitation Standard Operating Procedures (SSOP); recall procedures, and applicable supporting regulations, such as Good Manufacturing Practices. The plan should also include provisions for notification and integrated activities with local "first-responders" (fire, police, hazardous material teams, etc.) as well as local, state and federal agencies.

To be effective, the plan must also include an on-going employee-training program as well as frequent exercises.

Costs of Implementation

Implementation of food security plans will require outlays for equipment, materials and most likely additional personnel. State and Federal Legislatures could provide economic support and incentive for these expenditures by implementing a 10% Investment Tax Credit. Such credits have proven to be a

positive motivator for companies and a stimulus to the economy in general. The credit provides direct tax relief while requiring a 10:1 investment by the tax paying entity.

Employee Screening

In regards to human resources, the key to reducing and managing the treat to our food supply is a company's employees. The 9-11 incident has heightened the concern of agencies in regards to employees, particularly as may relate to documented or un-documented aliens or those in violation of visa restrictions. The emphasis, to date, by most regulating agencies has been directed toward requiring employers to conduct criminal background investigations of applicants and to collect copies of their work documents. On paper, this looks like a workable solution. In reality, it is not. While such a program can be quite expensive ($50 - $1000 per employee), the information garnered is seldom complete. Furthermore, there is no effective infrastructure in the private sector to support such a program. To further complicate matters, employees are often severely restricted as to what information they can seek, and what resultant actions they may take, by employee and civil rights regulations, not to mention a rather justified fear of retaliatory litigation.

Even the Immigration and Naturalization Service (INS) currently lacks an effective protocol for verification of an alien's work status or even an integrated inter-agency program to identify and refuse entry to undesirable aliens. A radio show recently reported that Congressman Rick Larson (Washington 2d District) worked a three-hour shift with INS at the Blaine, Washington Crossing (NPR, 2002). He was reportedly dismayed to have to report that he had access up to 12 separate databases in verification of a single individual. Despite this, federal agencies have electronic access to immigration, criminal, associated state, local and federal records far better than any private company could hope to equal. Thus it would appear that a federal agency is in a much better position to conduct a meaningful, effective, and economic review of an employee's background and/or eligibility.

A solution to this situation, therefore, would be for the federal government to develop a single point entry, integrated database. This would be followed by the expansion of a test program currently being evaluated on a limited basis by the INS. Under that program, the INS is requiring employers in six states to submit employee's names, social security numbers, other documentation numbers, and supplemental information on prompt basis. The INS then conducts an electronic review of the employee's work status.

This proposal would require all employers within the food sector to electronically submit basic employee identification data, including a digital photo(s), of existing and potential employees to the designated agency within one business day of employment or determination to employ. The designated agency would be tasked

with promptly conducting an electronic review and reporting back to the employer electronically. Such a program would be conducted electronically via the Internet and require little agency employee interaction except for exception and validation purposes.

The inclusion of digital photos would further enhance the program. Digital photography and electronic transmission of digital files is both practical and economical. Further, there are several automated imaging technologies currently employed by law enforcement agencies, with many of them being recently implemented in response to the 9-11 incident.

A bill incorporated the above activities should identify the INS as the responsible agency and provide the funding to implement the program. The program would significantly improve the effectiveness of employee background checks and markedly enhance the security of the nation' food supply.

In the interim there is much that individual producers, processors and manufacturers can do to develop strategies for recognizing potential hazards, and measures that can be taken as part of a food safety program to reduce the risk of terrorism. One such strategy is to develop a program derived from familiar HACCP principles.

Development of a Food Security Plan Based Upon HACCP Principles

Each organization will be uniquely situated and should develop a sensible security plan for managing the risk of terrorism. Because different units and locations will most likely have different risks, each should be evaluated separately. Critical factors for developing a plan will include evaluating specific hazards, determining the relative risk, and evaluating economic realities associated with managing this risk. There is a strong parallel between developing a preventive strategy for a terrorist attack and the elements of a Hazard Analysis Critical Control Point (HACCP) plan (*see for example*, 21 CFR Part 123). The emphasis here, as with HACCP, is placed *preventive* and not *reactive* measures. HACCP is a systematic approach to the identification, evaluation, and control of food-safety hazards (Anon, 1997).

Fundamental to an effective security plan is that it be built upon a foundation that includes and integrates an effective HACCP plan, the following of Good Manufacturing Practices or GMPs (21 CFR Part 110), and execution of a Sanitation Standard Operating Procedures in accordance with 21 CFR §123.11).

Personal safety, prevention of kidnapping of employees and/or their families, and defenses against armed attacks are not included within the scope of this paper. Rather, concentration is more directed toward protecting the integrity of the food produced and the systems employed in such production. Suffice it to say there are

many overlapping elements and basic to all is controlled access and limitation of opportunity.

Evaluating Security Risks and Identifying Hazards

Initially, a company or organization should complete an analysis of its facilities and operations to identify significant hazards, the potential exposure to a particular hazard, and evaluate the risks of an occurrence. This analysis should not be limited to just the production facility nor at peak operations, but should include the entire scope of operations including suppliers, receiving, processing lines, sub-contracting facilities, materials and goods-in-process holding, packaging, warehousing, rolling stock, distribution, physical plant, etc. as well as research center, farm and /or ancillary site security. It should also include raw materials and distribution handled by common carrier or third parties. Water sources and supplies may well be of specific concern, particularly if water is used as an ingredient or comes in direct contact with consumable products. In effect, a "Chain-of-Custody" concept should be employed from the farm to the table.

It is recommended that the team concept be used in developing such a plan. In larger organizations, this may actually consist of a series of teams formed within identifiable units. Regardless of the structure, good leadership and a comprehensive integration of the team's, or teams', recommendations are critical factors as is the buy-in of the resultant program by both management and employees at all levels.

Managing the Risk – Preventive Measures

Since it will probably be impossible to eliminate all hazards, a reasonable procedure must be instituted to manage them. Probably the best strategy is to develop preventive or risk control measures that would reduce or eliminate any significant hazards. As part of this, we recommend that you determine points in your operation which are critical for controlling the security risks you have identified. These points may change during the course of a day, or seasonally. They may also shift with product manufactured, with suppliers, distribution systems or end user.

Then, establish a monitoring procedure for these risk control points (similar to what you may already have in place for monitoring critical control points in a HACCP plan). Along with protocols should be corrective actions (again, similar to what you may have in place as part of your HACCP program). A plan for verifying the effectiveness of the preventive and risk controls measures in your food security plan should also be included. The use of forms such as the "HACCP Hazard Analysis Worksheet" or the "HACCP Plan Form" (FDA, 2001) may be of benefit in some cases.

Suggested Steps for Developing a Security Plan

Here are suggested steps for developing a security plan based upon an approach similar to that used in a HACCP plan:

1. Develop a comprehensive flow chart(s) that depict your firm's operations from primary production or receiving to consumption by the end user.

2. Examine each element to determine whether there are significant food security hazards and evaluate the likelihood of the risk of these hazards.

3. Determine the points in your operation that are critical for managing a specific risk. These could be locations, processes, functions, or times when your operation is at greatest risk.

4. Develop and institute preventive or risk control measures to reduce these hazards to acceptable levels.

5. Where appropriate, establish critical limits or restraints that are not to be violated or breached without a resulting corrective action being initiated.

6. Develop monitoring procedures for each critical point in your security plan. Monitoring is a systematic periodic activity to ensure that critical controls are in place and have not been breached or compromised in any way. These should be in writing. Test to see that your monitoring procedures are working and "workable" for your organization.

7. Develop a procedure similar to a corrective-action program under HACCP to fix security problems or failures that occur if a critical control has been breached or compromised. Ensure that the problems are fixed by rigorously retesting your system and its risk monitoring procedures. Then revise your plan to include any changes to the critical controls and/or monitoring procedures and to reduce the likelihood that a similar breach would happen again. Corrective actions may also include the prompt notification of appropriate authorities and the execution of ancillary steps such as an evacuation, lockdown or similar activity.

8. Periodically test or verify your security program to ensure that it works. Verification programs should be written as confidential protocols. Revising your written protocols when your operations or any key features of it change is vital. A change in your operations,

product form, suppliers, distributors, etc. may introduce or remove hazards and require that your plan be revised.

9. Above all, adequate and comprehensive records must be developed. These records should be handled as confidential. They should also be maintained to record monitoring, preventive measure, deviations, corrective action, and verification activities. Supporting documentation should also be incorporated into the records. These might include outside agency notification protocols, hazardous material information, media protocols, an employee notification plan, response team information, and recall procedures. Supervisory personnel, on a timely basis, must systematically and periodically review these records. The inclusion of superfluous and unnecessary documentation should be avoided.

An Application

A simple example of how two related elements (procurement of raw materials and transportation-in) for a food manufacturing operation using these principles is presented in **Appendix 1**.

Specific Suggestions

The key to a successful program is vigilance by management and all employees. Training is critical. A clear standard operating procedure must be developed and followed both for day-to-day operations, for suspicious incidents or individuals, and for actual attacks. The problems arising from an actual attack would be similar to what you may already have in a crisis management plan. If product safety is at issue, recall procedures would need to be followed. As with recall programs, individual farms, companies, or research institutions should periodically use exercises and drills to test whether a security plan is current, workable and effective.

Unfortunately cost will often be the controlling factor in development of a food security program since it is impossible physically and financially to guard against every eventuality. Not all of the recommendations included herein will be appropriate, practical, or economical for every individual entity. As with HACCP, food safety programs will be market driven. Only you can determine which are appropriate and should be implemented by your company.

Surveying Site

A good digital camera, access to plant plans, and aerial photos are excellent tools to use in developing your plan. Aerial photos may be obtained specifically for your operation or you may access them through your local county assessor's office or often times through your local County Extension Office. They may even

be available off the web from a number of state, federal and private sources. Consider using them, particularly since they are also readily available to the terrorists and they are not bashful about employing such technology.

Farming Operations

A farmer might well require certifications from seed, feed, livestock, fertilizer, pesticide and herbicide providers and periodically seeking third-party verification. We recommend that a grower avoid stockpiling hazardous materials, keeping the amount on site to a minimum, and to secure stores and applicator equipment. We also recommend that bin locks or other tamper evident device(s) be placed on feed bins and that the security of water delivery systems be evaluated.

Growers should develop monitoring and tracking protocols for harvests until they are safely transported and stored within a warehouse. To the extent practical, access to croplands and livestock should be controlled and restricted to appropriate personnel. Surveillance equipment is also an option; the cost of such equipment has decreased markedly in recent years. Access to animals at auctions and sales barns should be restricted and direct contact with animals tightly controlled. Consideration should also be given to: compartmentalizing livestock operations, improving hand washing/sanitation facilities, providing or improving clothes changing facilities for employees, improving equipment cleaning operations when animals are to be transported between two locations, and requiring foot and vehicle sanitation dips at critical access locations as ways of controlling the spread of a disease.

The Water Supply

Additional preventive measures concerning the safety of the water supply used within a food processing operation should be considered. Evaluating the security of wells, hydrants, storage and water handling facilities whether these are on-site or controlled by a municipality are prudent measures. Even if water is from a municipal source, the integrity of this supply ultimately falls upon the production facility.

Normally the water is your responsibility from the meter on, but don't hesitate to question your supplier. Many water suppliers are notoriously negligent in implementing even the basic security practices ranging from unsecured wells, standpipes, reservoirs, pumping stations open to the public to exposed distribution systems. Consider checking your water more frequently regardless of its source. Locating an alternate source of potable water, providing for additional on-site storage in case of emergency, or providing a backup water purification system may be also be desirable (FDA, 2002a). Precautions should also be taken to ensure that air entering the operation is not contaminated. This could include securing access and a routine examination of air intake points for physical integrity (FDA, 2002a).

Letters of Guarantee

Food processors should request letters of guarantee from suppliers and require protected transportation of ingredients. It would be prudent to revisit inspection programs for incoming ingredients including packaging materials, labels, and supplies used within the production facility and office. Specifically, do not accept unordered ingredients/ shipments or product received in opened containers or damaged. Require tamper-proof packaging or shipping containers as well as numbered seals. Also ensure, as part of your recall program, that you can track the use of any specific lot of an ingredient from receipt through production to final product and distribution. Work with your suppliers and common carriers to ensure that they have instituted appropriate food security programs. We suggest that you develop an audit program in this area similar to one you may already have as part of an existing food safety or food quality program. This should include periodic inspections by your organization or third-party experts of your vendor's systems including distributions systems.

Distribution and Transit

Controls during distribution and transit are important and preventive measures could include expanded use of tamper proof seals of containers with enroute monitoring. The seal alpha-numerics should be communicated electronically, separate from the shipment itself; with the numbers and seal integrity verified prior to opening the container, and retransmitted to the supplier upon receipt. Off loading should be conducted under controlled conditions with periodic testing a must. The integrity of finished products (including reconciling the amount received with amount ordered) should be controlled during storage and distribution (FDA, 2002a). Where appropriate, tamper proof or tamper evident packaging, at several levels, may be advised.

Chemical Safety

GMPS also require that hazardous materials be stored and handled properly to avoid contamination of food and food contact surfaces (21 CFR §§110.20(b)(2) & 110.35(b)(iv)(2)). Now would be a good time to revisit inventory control for hazardous materials (including ingredients), and the safety and security of storage areas (including use within the processing area itself). Access should be limited to hazardous materials to only those individuals who need to use these materials and who have proper training in handling them properly.

Employee and Contractor Screening

Employee and contractor screening have become increasingly important. We recommend that, where appropriate, a criminal background check should be conducted as a condition of employment and that contractors who have relatively open access to the facility (*e.g*. outside cleaning crews, pest inspectors) be held to

the same standards as employees. These checks can be expensive and, unfortunately, often do not give complete data. A suggestion might be that the Immigration and Naturalization Service, or other appropriate agency, expand and refine the current employment- eligibility program to provide a national and local agency check and reports the findings to the employer in a timely manner. This would be much more effective than tasking individual employers to accomplishing such checks.

Employers should also ensure that employee and sub/contractor rosters, job and shift assignments are current, reviewed on a weekly basis, and updated. We recommend that all employees/contractors wear photo ID while on the job and that badges be recovered when an individual is no longer on assignment. Such badges can be color coded, or otherwise identified, to indicate to which parts of the plant or operations that the individual has authorized access. They should also be periodically collected unannounced, accounted for, and reissued in a different format. We also recommend increasing the surveillance of contractors while on the job and implementing similar control measures. Employees or contractors should not be at the work site unless they are scheduled to be there (FDA, 2002a).

Personal Items

Under proper GMP procedures, no personal items such as lunches, purses, etc. should be permitted into a food processing area; you may wish to extend this procedure to prohibit any personal objects from entering the production facility at all. The FDA recommends that employees be provided with mesh lockers with employer issued locks (FDA, 2002a). A condition of employment is that the employer may inspect the personal property of an employee at any time.

Compartmentalizing Job Functions

We further recommend that job functions within a facility be compartmentalized. This will mean restricting access to any specific areas of the plant to only the individuals who need to be there. This could be done through the use of color-coded badges. Controlling access is particularly critical for operations processing ready-to-eat food products.

Keys and Identification

Ensure that you can account for all keys, that keys are have individual discreet numbers, and that keys are marked "do not duplicate." Better yet, consider the use of card-swipe electronic locks that eliminate the need for keys. Most of these systems not only allow you to control individual access, but also maintain a record when these individuals have gained entry. Individual access can also be controlled on a time basis, thus only permitting entrance during scheduled hours. ID badges commonly serve the dual purpose of also being the access card. Periodic unannounced inventories of keys should also be considered.

A special note should be made in regards to discharged employees. Security badges, keys, etc. should be immediately surrendered by the employee who should be promptly escorted from the facility and not be permitted to return to the facility except under escort as a controlled visitor. Discharges, whether they are simply the result of the end of a season, a reduction in work force, or a firing for cause, need to be handled carefully and with appropriate sensitivity.

Facilities Access

Reducing points of access to the plant should be considered (FDA, 2002a). This may include improving the security of and/or reducing the number of accessible doors, windows, hatches, trucks, railcars or bulk storage areas. The number of nooks and crannies that could be used to hide intentional contaminants either inside or outside the plant should be reduced. Emergency exit integrity and in appropriate numbers should be maintained with alarmed "Emergency Use Only" exits where appropriate.

Visitors and Inspectors

Individuals purporting to be inspectors should provide appropriate identification and be vetted by backup procedures such as a simple telephone call to the publicly listed telephone number of the visitor's parent agency. Such individuals should be escorted at all times within the plant. Consider a "no-photography" policy as a way of improving security and as a means of protecting intellectual property if this policy is not already in effect, experience or potential risk.

Access to processing areas including locker and break rooms by visitors (including truckers, delivery people, supplier representatives, customers, applicants for employment or other visitors) and employees should be strictly controlled both within the plant and between different areas of the plant. A check in procedure and issuance of visitor badges should be conducted in a reception area or another location that is not adjacent to the processing area.

All visitor badges should be accounted for on a daily, or otherwise appropriate, basis. Some firms will no longer accept visitors on-site or visitors who have not made appointments in advance. Where visitors and tours are an important part of public relations or marketing, visitors should be confined to viewing galleries, or at a minimum, be closely monitored and escorted at all times. All individuals with escort authority should be trained and be aware of the importance of their responsibilities.

Parking

Stricter control of parking at the facility may need to be instituted including parking permits and vehicle registration. Enclosing the parking area, increasing

physical security, no parking safe-zones, access and lighting, and/or instituting a vehicle inspection program may become necessary based upon prior policy in which all job applicants apply for positions at a location far removed from the processing facility. Initial screening and interviews of potential employees and contractors occurs off-site.

Research Institutions

Research institutions should also implement similar safeguards including controlled access to laboratories, test plots, and the supporting infrastructure. Increased security of, and access to, hazardous materials is advised. This would include locked access to dangerous biological materials or chemicals. A review of handling procedures for cleaning materials, solvents, acids, bases, paints, pesticides, water treatment and other chemicals used within a facility should be reviewed and access, handling and storage procedures revisited. For quality control labs in industry, lab access should be restricted to lab personnel only (FDA, 2002a). Under GMPS, dangerous materials should remain in the lab and not be brought into office or production areas. Assign responsibility for the inventory and control of dangerous materials (*e.g.* toxic reagents, bacterial cultures, drugs) to a specific individual. Have a plan in place for immediately investigating missing reagents or other potentially dangerous materials.

Quality Control Labs

Quality control labs can conduct random product and environmental testing as a preventive measure against contamination during the processing operation. For example, testing different portions than are normally sampled, *e.g*. sampling different regions of an animal carcass in addition to those proscribed by regulation, or by collecting samples at different times or different sampling locations. We also recommend that you contact local or regional food testing and forensic laboratories and learn what their capabilities are and develop a good working relationship with them.

Employee Vigilance

Employees should be made aware of their responsibilities to stay alert for and report suspicious activities, objects and persons at their workplace or at home. Responsibility for specific security functions should be assigned to qualified individuals and included within job descriptions. Food security training programs should be provided to employees with periodic updates which include how to prevent, detect and respond to a product tampering incident, terrorist activity or threat. This could be conducted in conjunction with HACCP and/or recall training or refresher programs. Sales personnel and others including distributors and retailers should be made familiar with your products and how they are packaged and distributed so that they may be able to detect whether a product has been altered or contaminated.

Security Checks

Security checks should be conducted on at least a daily basis. All employees and contractors should be trained to be vigilant for the presence of unidentified, unattended or unauthorized vehicles, the presence of containers in or near the facility, and unauthorized access (even to unsecured areas) by unidentified persons or employees who have no apparent reason to be there. Also, employees should be trained to look for signs of sabotage or tampering of equipment, products or ingredients, removal or tampering with product or worker safety features of equipment, or for signs of attempted unauthorized access to equipment.

In light of recent developments, it is prudent to have procedures in place for handling shipments to the facility including suspicious packages and mail. This could include securing mailrooms and instituting visual or instrument based package screening.

Emergency Evacuation Plans

Companies are required to have emergency evacuation plans in place. But when was the last time you tested it? These plans should be reviewed for appropriateness in consideration for potential biological or other terrorist threats. Management should file a copy of the company's safety and emergency procedures with the local municipal planning department and with emergency response agencies. However, these entities must be required to safeguard these documents and be ***prohibited from releasing them to any parties without your knowledge and written consent.*** An additional option is to have the evacuation plan along with the plant layout in a locked and sealed container outside the facility in case access to the facility is limited in an emergency.

Following the September 11 incidents, the Food and Drug Administration (FDA) contacted major food industry associations requesting that they advise their members to review current procedures and markedly increase vigilance (FDA, 2002a,b). The FDA, other governmental agencies, and some academic institutions can provide assistance in planning and response to real or suspected terrorist incidents. Since September 11, 2001, there has been a proliferation of consultants with purported expertise in this field. As with any such engagement, carefully evaluate actual and pertinent qualifications prior to employment.

If you think your organization has been or might be the target of a terrorist attack, seek immediate assistance from your local law enforcement and health/hazardous materials handling experts (often the fire department). Additional support can be provided by the Federal Bureau of Investigation (FBI) (National: 202/324-3000), US Department of Agriculture Office of Crisis Planning and Management

(877/559-9872, 202/720-5711), The FDA Emergency Operations Office (301/443-1240) and your state emergency management division.

Contact information for the relevant safety and law enforcement agencies should be readily available to employees and updated as needed. The FDA recommends that an organization have a capable media spokesman and generic press statements prepared in advance in case of an emergency (FDA, 2002a). In some states, such as Washington, National Guard units may have special training and equipment to respond to chemical or biological terrorist threats.

It is not possible to present a full picture of the bioterrorist threat to food production in such a short article, or to present every appropriate defense, let alone to address the full scope of terrorist threats including cyber, conventional, and economic terrorist acts. Suffice it to say that the threat is real and most likely these incidents will continue. Individuals, institutions, and companies can become more cognizant of the threat and take steps to reduce the likelihood and impact of any incident. This does not mean that paranoia should reign supreme. These risks, as with others tied to food safety, are manageable. We must keep the risk in perspective and insure that common sense prevails. As with HACCP and recall protocols, prior planning, training, and established procedures are essential tools.

REFERENCES

ACI, 2000. American Conference Institute. 2000. Product Tampering and Accidental Contamination Conference and Workshop. June 12-14, 2000. San Francisco, CA.

Anon., 1997. HACCP: Hazard Analysis and Critical Control Point Training Curriculum, North Carolina SeaGrant Publication UNC-SG-98-07, Raleigh, NC.

Anon. 2002. State legislative activity in 2001 related to agricultural biotechnology. Pew Initiative on Food and Biotechnology. http://pewagbiotech.org.

Bascetta, CA. 2000. Combating terrorism. Chemical and biological medical supplies are poorly managed. GAO/T-HEHS/AIMD-00-59. March 8, 2000. GAO-HEHS/AIMD-00-36. Oct. 29, 1999.

Bledsoe, G.E. and Rasco, B.A. 2002. Addressing the risk of bioterrorism in food production. *Food Technology*. In press.

Bledsoe, G.E. and Rasco, B.A. 2001. Terrorists at the Table Part II. Developing an Anti-Terrorism Plan. *Agrichemical and Environmental News*. Cooperative Extension. Washington State University, Tri-Cities November 2001. No. 187. pp 5-8.

Code of Federal Regulations. 2000. U.S. Government Printing Office. Washington DC.

FBI. 2000. FBI sponsors Genetic Engineering Ecoterrorism Conference in Berkeley, CA. January 26, 2000. FBI, National Institute of Justice, Berkeley and Davis Police Departments.

FEMA. 1998. Terrorism in the United States. Fact sheet. Federal Emergency Management Agency, Jan. 10, 1998. Washington, DC.

Food and Drug Administration. 2001. Fish & Fisheries Products Hazards & Control Guides; 3nd Ed., Department of Health and Human Services, Center for Food Safety and Applied Nutrition. Office of Seafood. Rockville, MD.

Food and Drug Administration. 2002a. Guidance for Industry. Food Producers, Processors, Transporters and Retailers: Food Security Preventive Measures Guidance. www.fda.gov.

Food and Drug Administration. 2002b. Guidance for Industry. Importers and Filers. Food Security Preventive Measures Guidance. www.fda.gov

Hollingsworth, P. 2001. Know a crisis when you see one. *Food Technology*. 54(3):24.

Miller, J., Engelberg, S. and Broad, W. 2001. Chapter 1 – The Attack, *Germs – Biological Weapons and America's Secret War*, Simon & Schuster, NY.NY. Pg 15-24

National Public Radio, 2002. All Things Considered, February 1, 2002.

Washington, 2001. Eco-terrorism. Public Hearing. June 11, 2001. Washington State Senate. Senate Judiciary Committee. PO Box 40466, Olympia, WA. 60pp.

Appendix 1
Example Using Raw Materials and Transportation-in for a Soft Drink Syrup Manufacturer

In this example, only two functions have been evaluated for illustrative purposes. The first function involves raw materials provided by an outside vendor. The second function involves the shipping the raw materials into the plant via common carrier. The primary biological terrorist threat in both cases would be that of purposeful contamination. The soft drink manufacturer deems the hazard to be significant. This is a judgment call. In the first case, the purchaser could require certification by the vendor as to the purity of individual lots. Further the materials would be required to be packaged in tamper proof packaging. Periodic, random product testing could also be accomplished at receiving as a check.

The vendor would be responsible for insuring the product is properly placed in the transporting equipment, whether it is a railcar, tanker, trailer, container, etc. The vendor would then supervise the sealing of all access to the product including doors (including in some cases inspection doors on vans or refers), vents, discharge ports, etc. Locks should also be used where practical. The vendor records all seal numbers and locations and forward this information electronically to the purchaser.

In some instances, temperature data recorders may be placed in the cargo or cargo area and can give an indication of unauthorized access (by temperature spikes) in addition to recording normal product temperature profiles. Integral temperature monitors are often integrated with automated on-board systems that can remotely notify a shipping company of an unusual condition.

Many private and common carrier fleets are now equipped with sophisticated, automated trip loggers/recorders that are integrated with the critical elements of the vehicle and Global Positioning Systems. These systems not only identify individual drivers, monitor vehicle speeds, van temperatures, and engine performance, but also compare vehicle locations, routes, and times against that scheduled. Some even monitor the physical condition of the driver. Normal operating information, as well as deviations that might indicate hijackings, unauthorized stops, or driver distress are automatically transmitted via satellite communication to the parent company. In many cases, they can also communicate directly with the nearest law enforcement agency.

It is entirely practical and possible for the receiving company to match the data output from even the simpler of these devices against schedule profiles. Many modular containers also have integral solid-state devices that may be used to monitor and record activities related to a particular unit. Data from these should be used as part of a security program when available.

The key to insuring that shipment integrity has been maintained is inspection at receiving. Product that does not meet the critical limits established by the purchasing firm should be rejected, isolated, and the vendor notified immediately. The receiving records and supporting documents should be reviewed in a timely manner by a qualified supervisor for every shipment.

At receiving, vendor certification and lot numbers should be matched against that provided by the vendor, normally through the purchasing department of the purchasing company. Volumes and weights should also be compared and matched against purchasing documents. In a similar manner, receiving as well as other personnel at all stages of production should inspect packaging integrity.

The receiving department should have the appropriate seal numbers available to them. As previously stated the vendor should send these electronically. The driver or other delivery agent should have this same data and use it periodically for inspection while transporting the materials, *but should not provide the data to receiving*. Seals and locks should not be removed until immediately prior to unloading. This is an example of simple job-function compartmentalization.

The printout from the truck recorder (often this will be provided electronically by the common carrier's company electronically from remotely downloaded data) should be examined for indications of unauthorized deviations.

While such measures as described in this example may appear onerous at first glance, many of the steps are simply accounting, quality control, and production records commonly in use. Many are just good business practices that should be employed regardless of a perceived bioterrorist threat.

Example: Production of Soft Drink Syrup
Hazard Analysis Worksheet

Item, Step or Function	***Identify Potential Hazards Introduced, Controlled, or Enhanced at this Step***	***Are Any Hazards Significant?***	***What Control Measure(s) Can be Applied to Prevent the Significant Hazard***	***Is this Control Measure Critical?***
Raw Materials	Purposeful Contamination	Yes	Certification of lot by vendor Tamper proof packaging Periodic testing	Yes Yes No
Transportation-In	Purposeful Contamination	Yes	All openings, vents, doors etc. locked and sealed by vendor. Data recorder included in shipment Automated trip recorder/report Vehicle held in secured facility when unattended.	Yes Yes Yes No

Firm Name: ***All-Good Syrups***
Address: 12 Baker St
London, CT

Prepared by: Conan Doyle
Date: January 15, 2002

Product Line/Description:
Drink Syrups

Intended use and consumer:
Commercial Bottlers